Surveillance Solution – How To Do It?

Grandstream has a full series of products for VoIP, Video and Surveillance. This article explains how to configure a surveillance solution for residential users or small enterprise users.

The main purpose of such application is to ENHANCE your alarm system, avoid the unnecessary false alarm which could be expensive because of law enforcement involved (just two or three such false alarm will cover the cost of the whole equipment investment). Also in some degree, this solution will help user to reduce the re-occurring monthly charge of security service.

Pre-Request:

1) **Home Computer Network and PSTN line (similar POTS line)**
2) **HT503 and GXV3615 (or ANY model of Grandstream surveillance product)**
3) **Smartphone with Internet connection**

Configuration

The solution is based on IP or computer network, therefore static IP is suggested. If the router used support static DHCP, then DHCP can also be used as long as the IP will NOT change after the router and device reboot.

Assume the user already has a home computer network or LAN in the office and no SIP server or proxy involved in such solution. If any SIP server or Proxy involved, the setting will be different although the principle is similar.

Following is the configuration for the equipment involved. We recommend user to use the default setting and ONLY change the parameters mentioned before. For used device, a factory reset is required to make the application running smoothly.

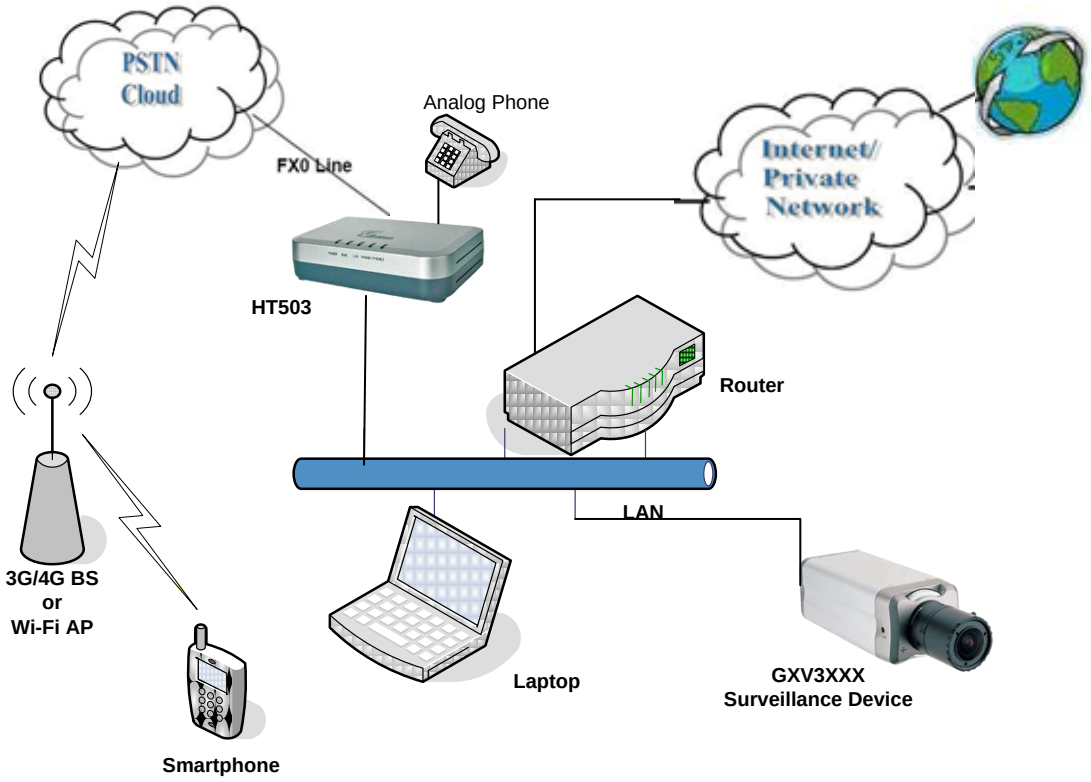


Figure 0: Application Network Schema

1. HT-503 Scenario

The HT503 is the key device here to connect the IP to PSTN world. The motion trigged alarm from surveillance camera is converted to a call sent out via HT503 to the user desired PSTN number, like cell phone.

User will hear siren when receiving the call. If email is configured in the surveillance device, a snapshot JPEG image will be sent to user configured email address.

User can immediately check back to see whether this is a true alarm by taking following actions:

1) Using browser (via Smartphone or PC) to check the snapshot of the camera (Smartphone) or live video stream (PC).*
2) Call back via the same PSTN number to deterrent if speaker is connected to the camera.
3) Call law enforcement for help if required. (no false alarm now)

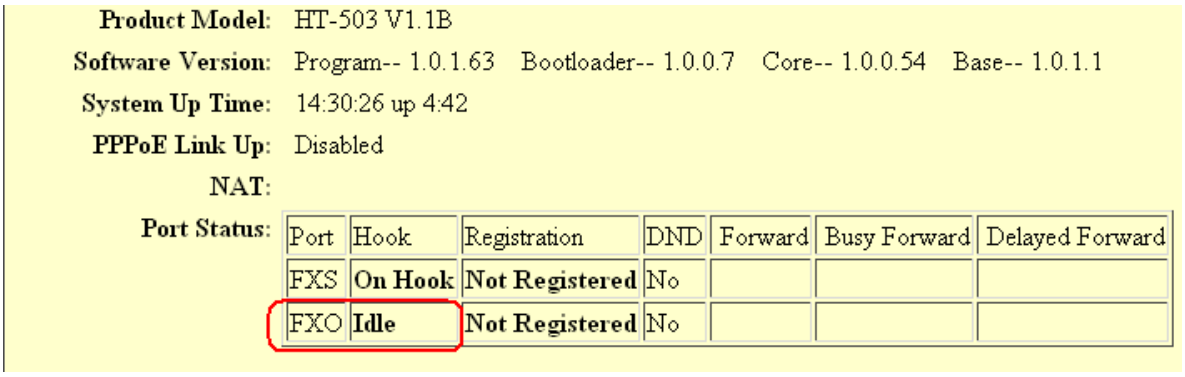
* Necessary configurations required in the router, like port forwarding, or DDNS service subscription.

Adjust and configure only following settings mentioned below and leave all other field using default setting.

Static IP is required in such application. User can follow HT503 user manual by using analogue phone and the built-in IVR of HT503 to key in IP address manually.

When PSTN line connected to the LINE port of the HT503, the status page should show as below (Figure 1-1). The FXO port will show “Idle” meaning the line is ready to calls.

Figure 1-1: HT503 Status Page


Product Model: HT-503 V1.1B
Software Version: Program-- 1.0.1.63 Bootloader-- 1.0.0.7 Core-- 1.0.0.54 Base-- 1.0.1.1
System Up Time: 14:30:26 up 4:42
PPPoE Link Up: Disabled
NAT:
Port Status:
Port Hook Registration DND Forward Busy Forward Delayed Forward
FXS On Hook Not Registered No
FXO Idle Not Registered No

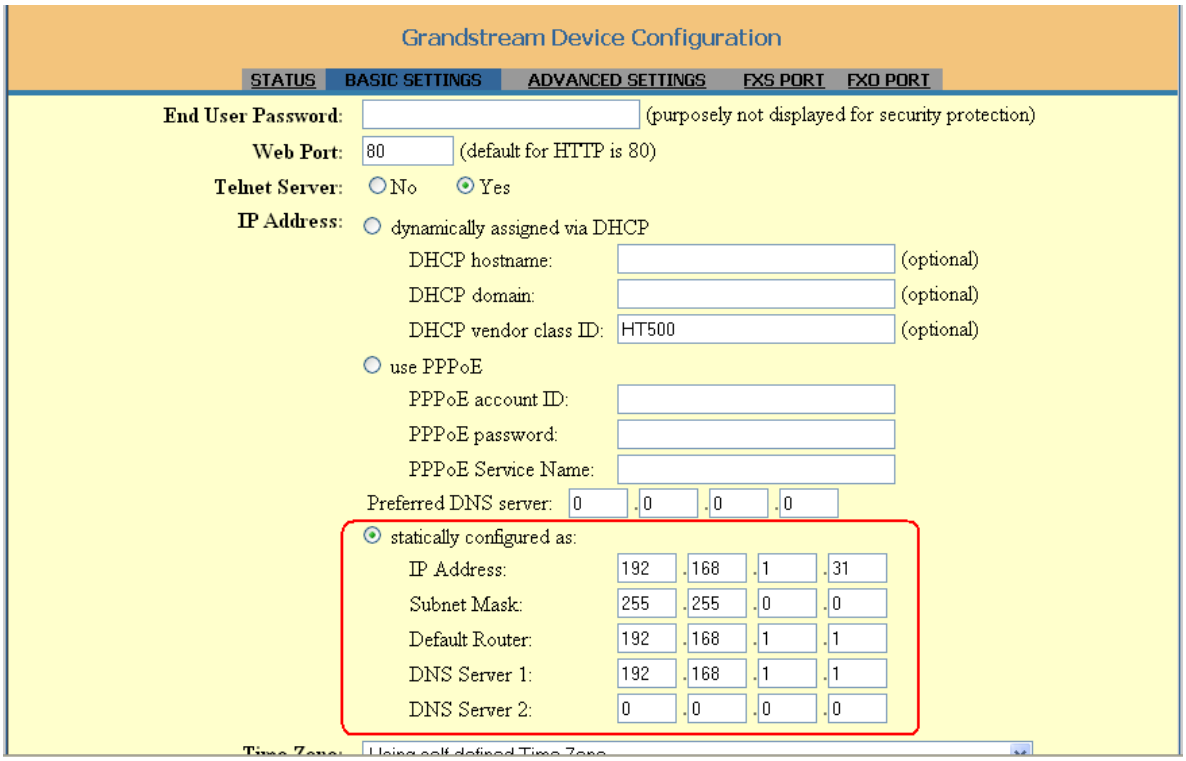
Below (Figure 1-2) is the sample Static IP configuration in the “BASIC SETTINGS” tag of HT503. User can use DHCP to get IP and change to static IP (if the router does not support Static DHCP) or follow user manual to use analogue phone and IVR to key in IP.

NOTE:

Make sure **NO IP DUPLICATION** in the network when using static IP otherwise none will work.
In this example setup, the IP address is as following:

HT503: **192.168.1.31 (WAN port IP, connect to one of the Router’s LAN ports)**
GS Surveillance Box: **192.168.1.30**
Router: **192.168.1.1**

Figure 1-2: HT503 IP Configuration



Below (Figure 1-3) is the alarm call related configuration:

- *Unconditional Call Forward to PSTN*: This is the place to fill in the number alarm call should be sent to (usually cell phone number). Fill in with exactly the same digits when dialing with that line using analogue phone, including dial prefix, area code, etc, in required by the PSTN carrier.
- *PIN for PSTN-to-VoIP Calls*: This is optional, if user want to call back and having speaker system connected to the camera, here is the PIN required to prevent any calls hit the system.
- *Unconditional Call Forward to VoIP*: The SIP Server field has to be the IP of the surveillance device, with port 5060, see below.

Figure 1-3: HT503 Alarm Call Number Setting

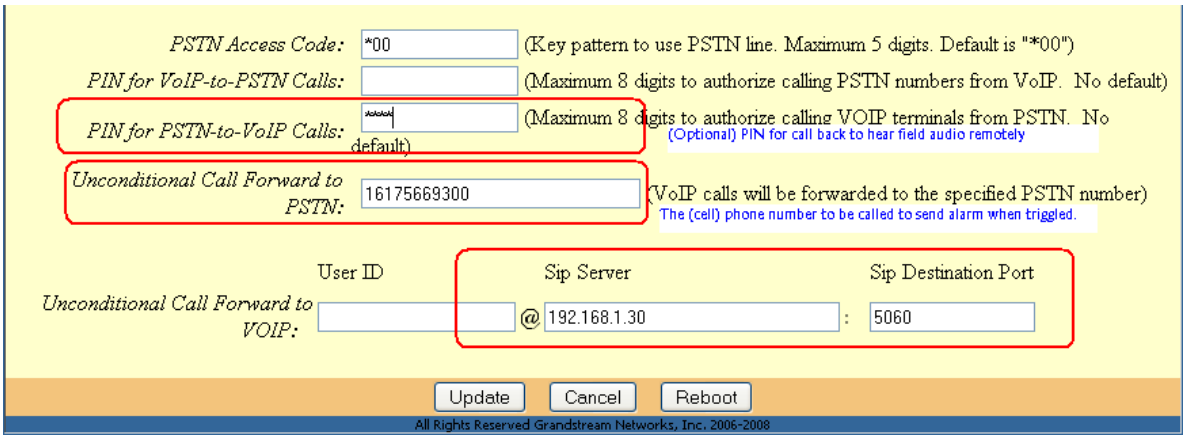

PSTN Access Code:
*00
(Key pattern to use PSTN line. Maximum 5 digits. Default is "*00")
PIN for VoIP-to-PSTN Calls:
(Maximum 8 digits to authorize calling PSTN numbers from VoIP. No default)
PIN for PSTN-to-VoIP Calls:
(Maximum 8 digits to authorize calling VOIP terminals from PSTN. No default)
(Optional) PIN for call back to hear field audio remotely
Unconditional Call Forward to PSTN:
16175669300
(VoIP calls will be forwarded to the specified PSTN number)
The (cell) phone number to be called to send alarm when triggled.
User ID
Sip Server
Sip Destination Port
Unconditional Call Forward to VOIP:
@
192.168.1.30
:
5060
Update
Cancel
Reboot
All Rights Reserved Grandstream Networks, Inc. 2006-2008

Figure 1-4: HT503 FXO Port Configuration

Below (Figure 1-4) is the FXO Port related configuration. Please configure only the mentioned parameters and do not change and leave all other parameters as default:

- **Account Active:** **Yes**
- **SIP User ID:** *Use any digits you want. HT503 just need some digits here to send to surveillance box therefore you can put ANY digits here. Here "110" is used as example.*
- **SIP Registration:** **NO**
  This is very important as there is NO SIP Server involved and we just manipulate the IP of each other device to make them work with each other.
- **Outgoing Call w/o Registration:** **YES**
  This is important also because NO SIP Server therefore no credentials involved here. The application is assumed in a secure and trusted LAN environment.
- **Local SIP Port:** **5062**
  This is the port HT503 FXO port will listen to.

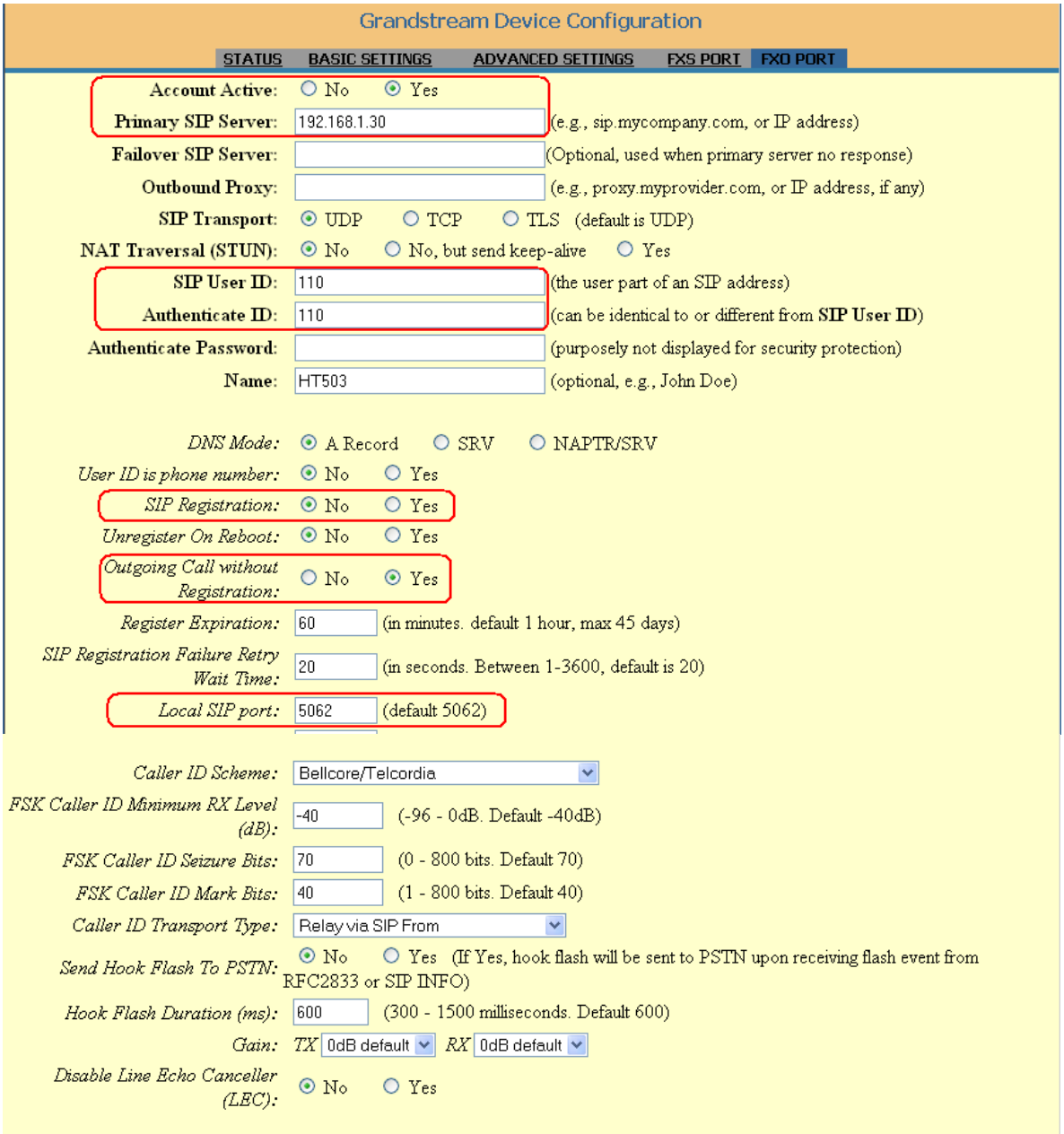

Grandstream Device Configuration
STATUS
BASIC SETTINGS
ADVANCED SETTINGS
FXS PORT
FXO PORT
Account Active: No Yes
Primary SIP Server: 192.168.1.30 (e.g., sip.mycompany.com, or IP address)
Failover SIP Server: (Optional, used when primary server no response)
Outbound Proxy: (e.g., proxy.myprovider.com, or IP address, if any)
SIP Transport: UDP TCP TLS (default is UDP)
NAT Traversal (STUN): No No, but send keep-alive Yes
SIP User ID: 110 (the user part of an SIP address)
Authenticate ID: 110 (can be identical to or different from SIP User ID)
Authenticate Password: (purposely not displayed for security protection)
Name: HT503 (optional, e.g., John Doe)
DNS Mode: A Record SRV NAPTR/SRV
User ID is phone number: No Yes
SIP Registration: No Yes
Unregister On Reboot: No Yes
Outgoing Call without Registration: No Yes
Register Expiration: 60 (in minutes. default 1 hour, max 45 days)
SIP Registration Failure Retry Wait Time: 20 (in seconds. Between 1-3600, default is 20)
Local SIP port: 5062 (default 5062)
Caller ID Scheme: Bellcore/Telcordia
FSK Caller ID Minimum RX Level (dB): -40 (-96 - 0dB. Default -40dB)
FSK Caller ID Seizure Bits: 70 (0 - 800 bits. Default 70)
FSK Caller ID Mark Bits: 40 (1 - 800 bits. Default 40)
Caller ID Transport Type: Relay via SIP From
Send Hook Flash To PSTN: No Yes (If Yes, hook flash will be sent to PSTN upon receiving flash event from RFC2833 or SIP INFO)
Hook Flash Duration (ms): 600 (300 - 1500 milliseconds. Default 600)
Gain: TX 0dB default RX 0dB default
Disable Line Echo Canceller (LEC): No Yes

Figure 1-5: HT503 FXO Port Configuration (Continued)

Below (Figure 1-5) is the FXO Port related configuration continued. The example below is using United States Bell Standard. If the HT503 is applied to other region, user is required to check with local carrier to search for the correct setting to make sure the HT503 function correctly.

- Number of Rings: This is for inbound calls (e.g.: from cell phone) to the PSTN connected to the HT503 be forwarded to the surveillance device where a speaker system is connected. User can determine how many rings the speaker system will pick up (be aware the likely conflict with voicemail if the VM is enabled in that line). PIN is suggested for such inbound call for security reason to avoid any calls hit the speaker.
- Wait for Dial Tone, 2 Stage Dialing suggested.

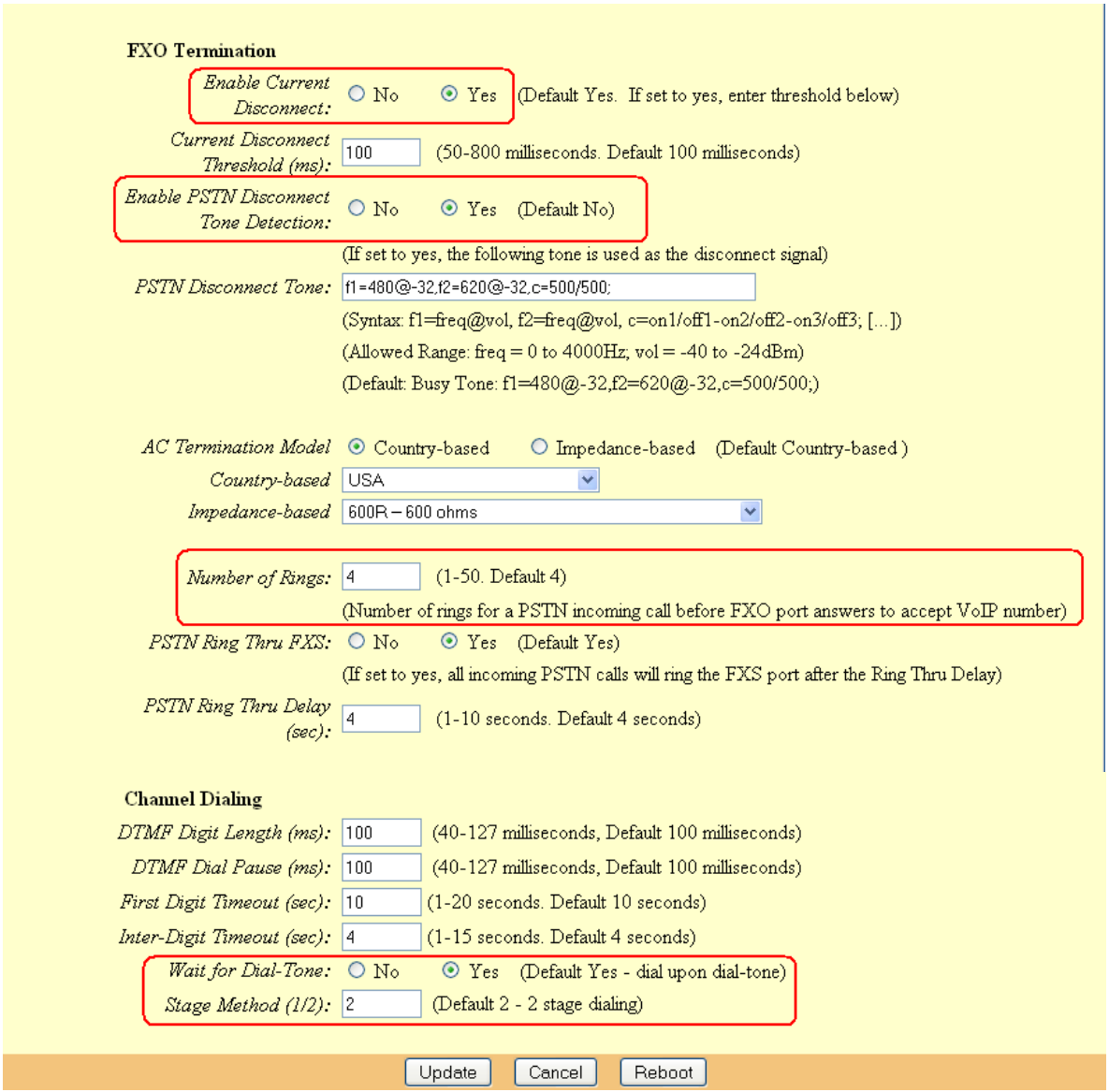
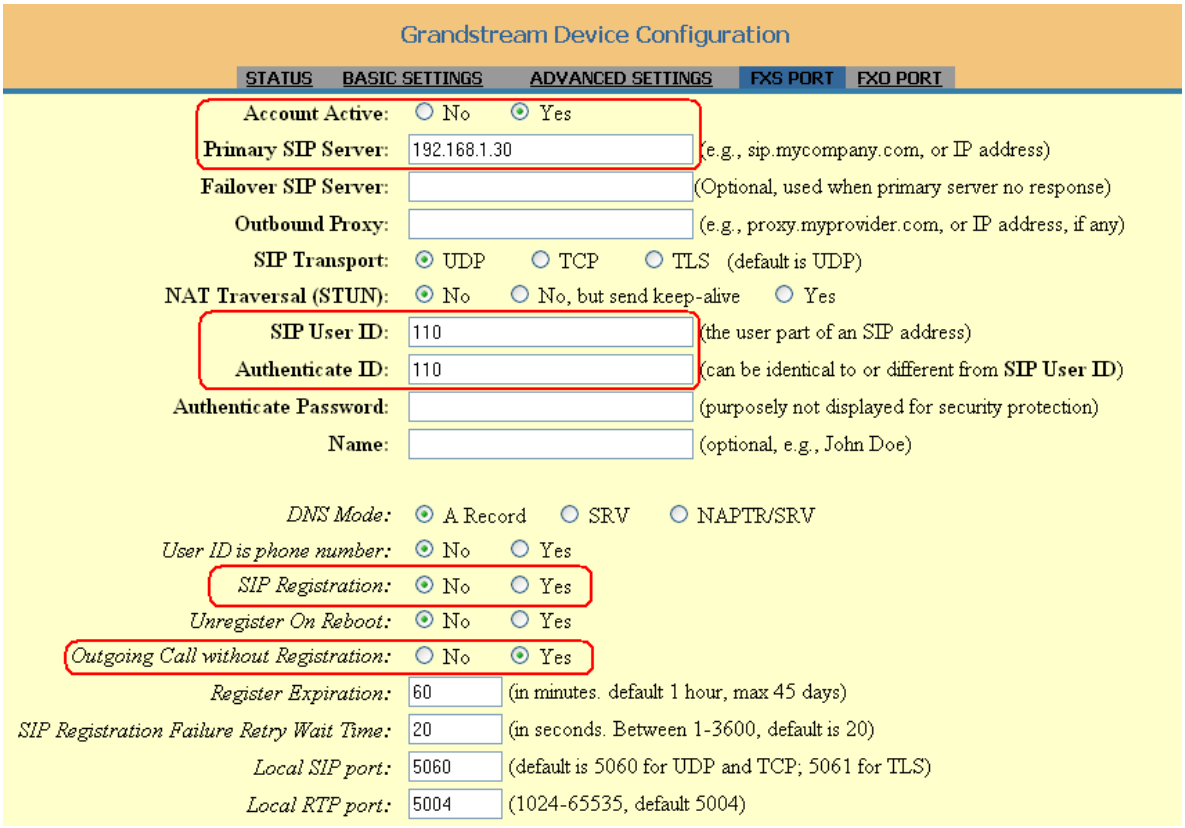

FXO Termination
Enable Current Disconnect: No Yes (Default Yes. If set to yes, enter threshold below)
Current Disconnect Threshold (ms): 100 (50-800 milliseconds. Default 100 milliseconds)
Enable PSTN Disconnect Tone Detection: No Yes (Default No)
(If set to yes, the following tone is used as the disconnect signal)
PSTN Disconnect Tone: f1=480@-32,f2=620@-32,c=500/500;
(Syntax: f1=freq@vol, f2=freq@vol, c=on1/off1-on2/off2-on3/off3; [...])
(Allowed Range: freq = 0 to 4000Hz; vol = -40 to -24dBm)
(Default: Busy Tone: f1=480@-32,f2=620@-32,c=500/500;)
AC Termination Model Country-based Impedance-based (Default Country-based)
Country-based USA
Impedance-based 600R – 600 ohms
Number of Rings: 4 (1-50. Default 4)
(Number of rings for a PSTN incoming call before FXO port answers to accept VoIP number)
PSTN Ring Thru FXS: No Yes (Default Yes)
(If set to yes, all incoming PSTN calls will ring the FXS port after the Ring Thru Delay)
PSTN Ring Thru Delay (sec): 4 (1-10 seconds. Default 4 seconds)
Channel Dialing
DTMF Digit Length (ms): 100 (40-127 milliseconds, Default 100 milliseconds)
DTMF Dial Pause (ms): 100 (40-127 milliseconds, Default 100 milliseconds)
First Digit Timeout (sec): 10 (1-20 seconds. Default 10 seconds)
Inter-Digit Timeout (sec): 4 (1-15 seconds. Default 4 seconds)
Wait for Dial-Tone: No Yes (Default Yes - dial upon dial-tone)
Stage Method (1/2): 2 (Default 2 - 2 stage dialing)
Update
Cancel
Reboot

Figure 1-6: HT503 FXS Port Configuration (Optional)

Below (Figure 1-6) is the optional FXS Port related configuration. The user can connect an analogue phone to the FXS port of the HT503, and use that phone (by dialing ANY digits followed by "#' key) to call and monitor the audio near the surveillance device installed.

If user has Grandstream video phone (like GXV3140 or GXV3000), user can configure the video phone using settings similar to this HT503 FXS Port to make the related GS video phone a live monitor device on demand. (Separate document will be provided for the configuration)


Grandstream Device Configuration
STATUS
BASIC SETTINGS
ADVANCED SETTINGS
FXS PORT
FXO PORT
Account Active: No Yes
Primary SIP Server: 192.168.1.30 (e.g., sip.mycompany.com, or IP address)
Failover SIP Server: (Optional, used when primary server no response)
Outbound Proxy: (e.g., proxy.myprovider.com, or IP address, if any)
SIP Transport: UDP TCP TLS (default is UDP)
NAT Traversal (STUN): No No, but send keep-alive Yes
SIP User ID: 110 (the user part of an SIP address)
Authenticate ID: 110 (can be identical to or different from SIP User ID)
Authenticate Password: (purposely not displayed for security protection)
Name: (optional, e.g., John Doe)
DNS Mode: A Record SRV NAPTR/SRV
User ID is phone number: No Yes
SIP Registration: No Yes
Unregister On Reboot: No Yes
Outgoing Call without Registration: No Yes
Register Expiration: 60 (in minutes. default 1 hour, max 45 days)
SIP Registration Failure Retry Wait Time: 20 (in seconds. Between 1-3600, default is 20)
Local SIP port: 5060 (default is 5060 for UDP and TCP; 5061 for TLS)
Local RTP port: 5004 (1024-65535, default 5004)

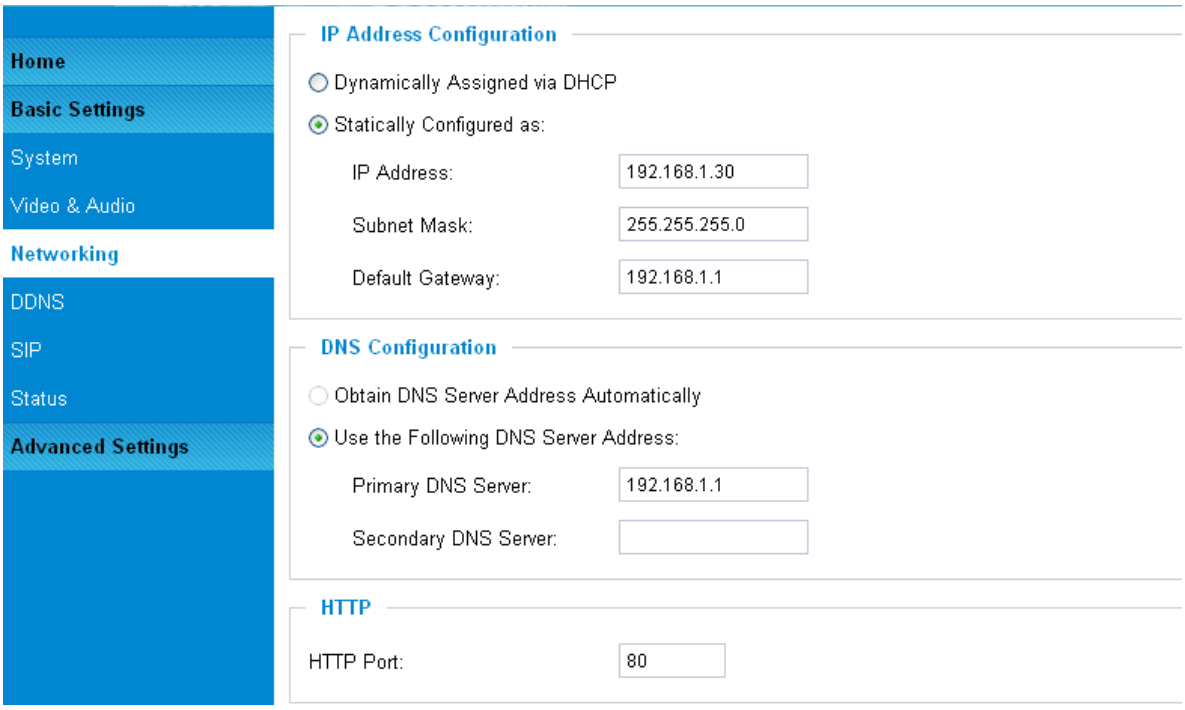
2. Surveillance Device Scenario (GXV3XXX IPC or DVS)

As mentioned previously, static IP is required in such application unless the router support static DHCP. This will prevent IP address change once the router or the device rebooted; also if port forwarding will work correctly only if the IP address is fixed or static.

Below (Figure 2-1) is the screenshot showing user how to configure the IP address to the Grandstream IP Surveillance products. Here we use GXV3615 as example and the IP address used in this example is:

GXV3615: 192.168.1.30

Figure 2-1: IP Address Setting of Surveillance Products



Below (Figure 2-2, 2-3) is the screenshot showing the SIP configuration in the Grandstream IP Surveillance products. All Grandstream IP Surveillance products share the same SIP stacks therefore the configurations are similar.

Because there is NO sip server involved and we are manipulate the IP to make peering operation, therefore the red “Offline” remark can be ignored.

NOTE:

1) *Port 5062 is important as HT503 FXO port is listening using this port.*
2) *User ID can be ANY digits as no SIP server credential exists.*
   Just use it as space taker. e.g.: “110” is used in the example.
3) *Phone List is the number the call should be sent. Space taker used as all the alarm calls will be send to HT503 FXO port to call out via the PSTN line to the pre-configured (cell) number.*

Figure 2-2: SIP Configuration of Surveillance Products

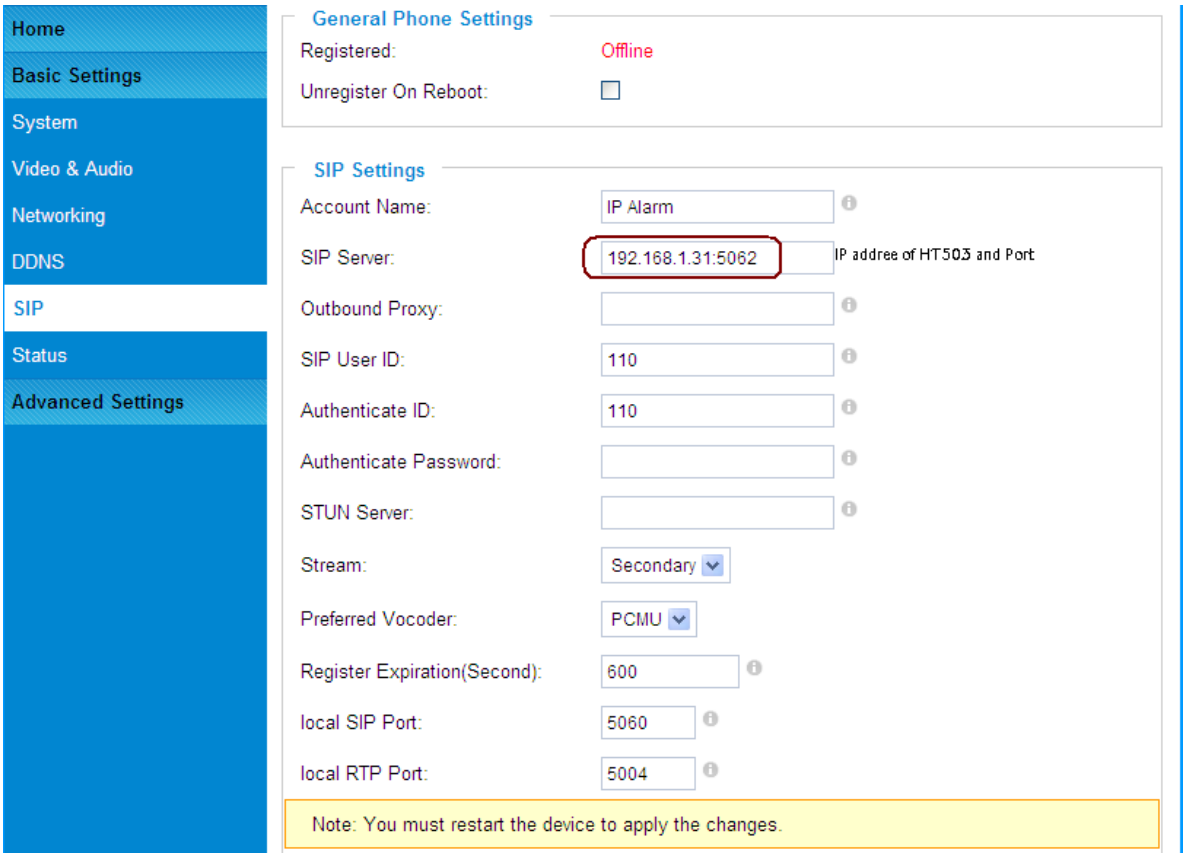
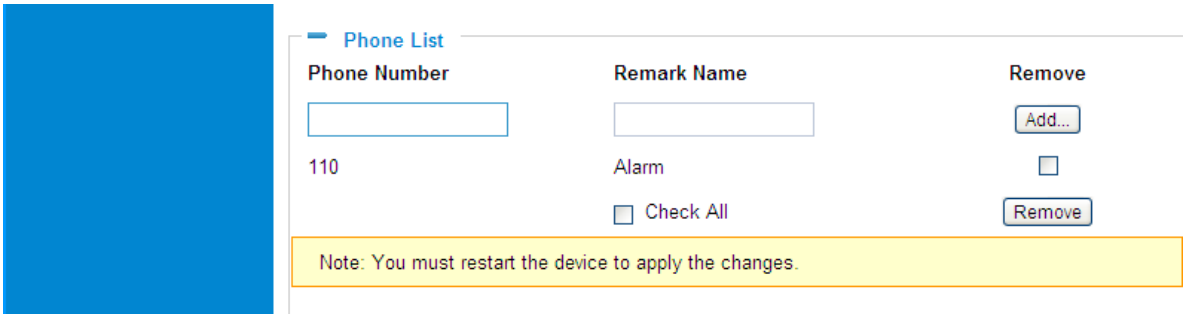


Figure 2-3: SIP Configuration of Surveillance Products



The “Phone List” is the place to fill real phone number if the Surveillance products have the related SIP server and registered. In this application, there is NO SIP server and only IP Peer Call solution, therefore any digits should be fine here as space taker to make it work.

Below (Figure 2-4, 2-5) is the screenshot of how to configure the Motion Detection of the Grandstream Surveillance product to work as desired:

NOTE:

1) Configure the “region” where monitor required. (Detailed steps please refer to related User Manual)
2) “Voice Alarm to SIP Phone” should be checked to allow outbound calls trigged by alarm. (Additional configuration required in SIP part, see also Figure 2-2 and 2-3).
3) “Email JPEG” checked only user want to receive emailed snapshot the moment alarm trigged. (Additional configuration required in SMTP part, see also Figure 2-6)
4) “Motion Detection Time Schedule” is configured to set the desired time span where the monitor working. The time is measured in 24 hour span from 00:00 to 23:59; therefore mid-night span will require two configurations to cover the time frame.

Figure 2-4: Motion Detection Configuration

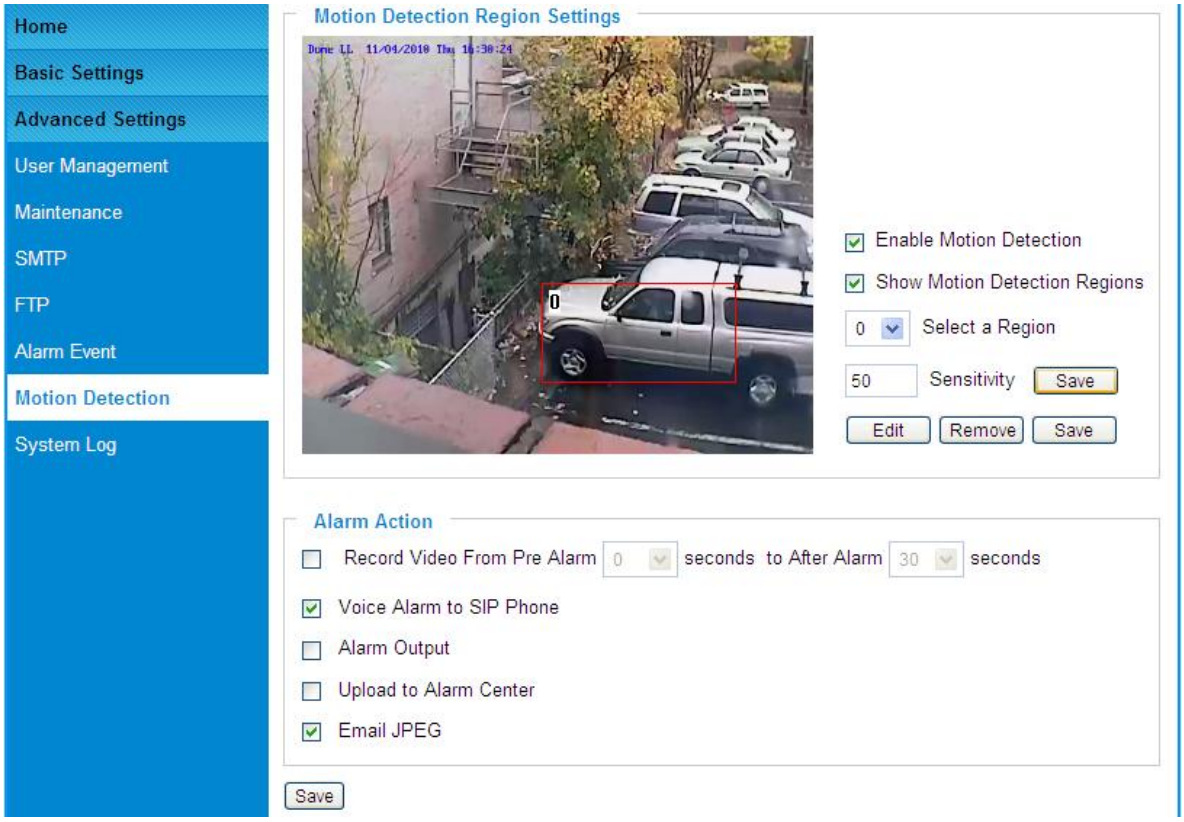
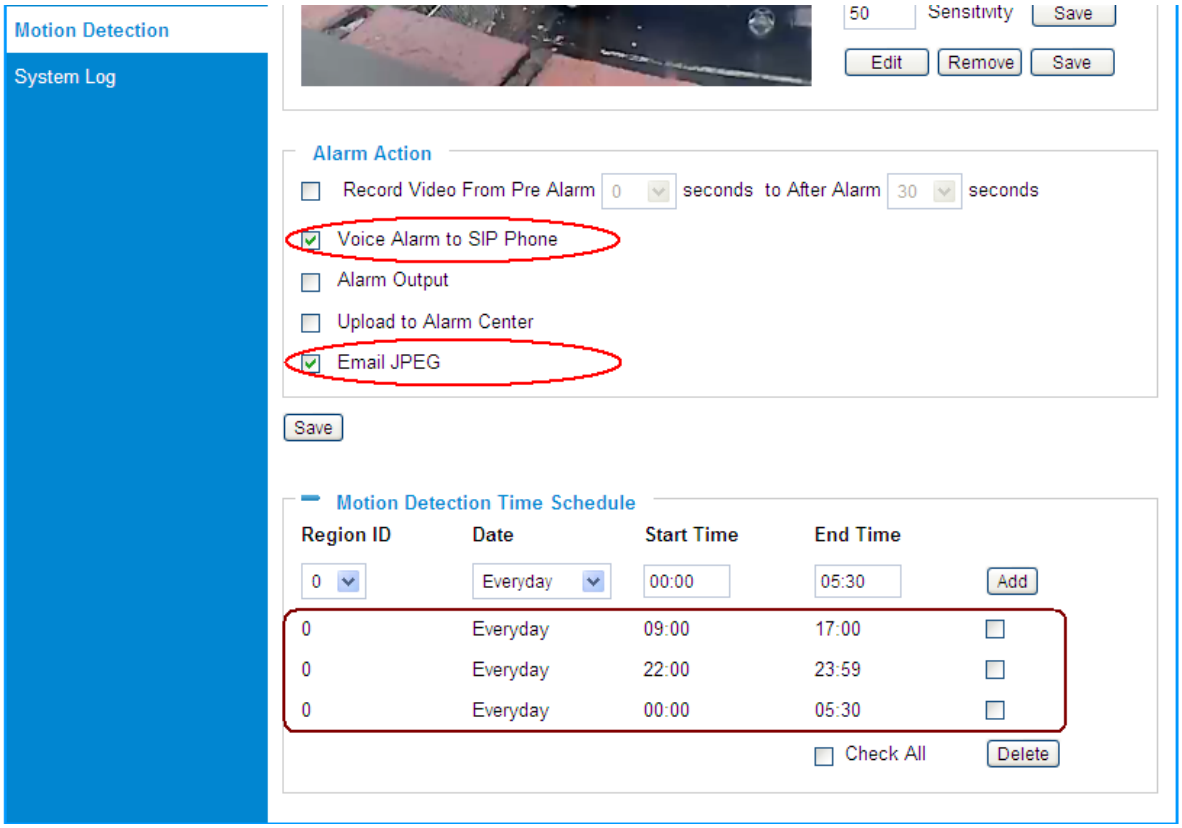


Figure 2-5: Motion Detection Configuration



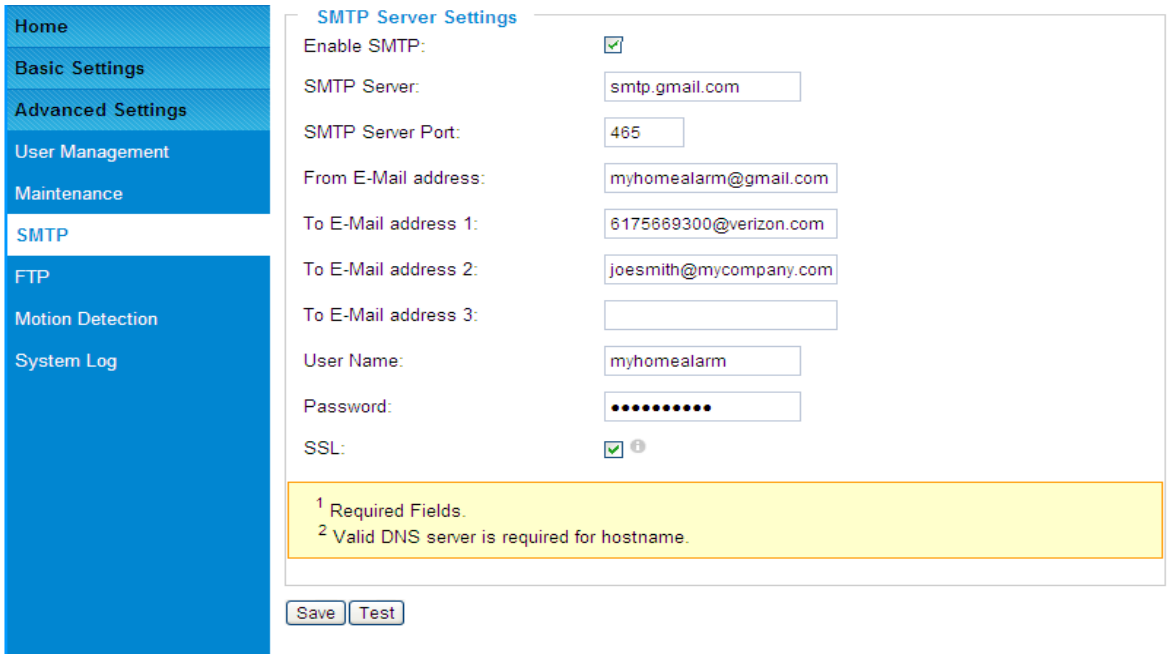
If user wants to receive the email with JPEG snapshot attached showing the moment alarm trigged, the correct SMTP setting should be configured in the Surveillance products.

Below is the example showing the configuration. In this example, Google's free Gmail setting is used. Customer can adjust this based on the actual email server setting.

Please consult with your network system administration for this par if using corporate email.

Once configured with the correct email credential, customer can click the "Test" icon to check whether the configuration is working correctly or as expected.

Figure 2-6: SMTP Setting



Verification

Once the alarm trigged, the user will get calls from this setup. Alarm will be trigged by Surveillance camera and calls will be made by the HT503 using the PSTN line connected to the “Line” Port.

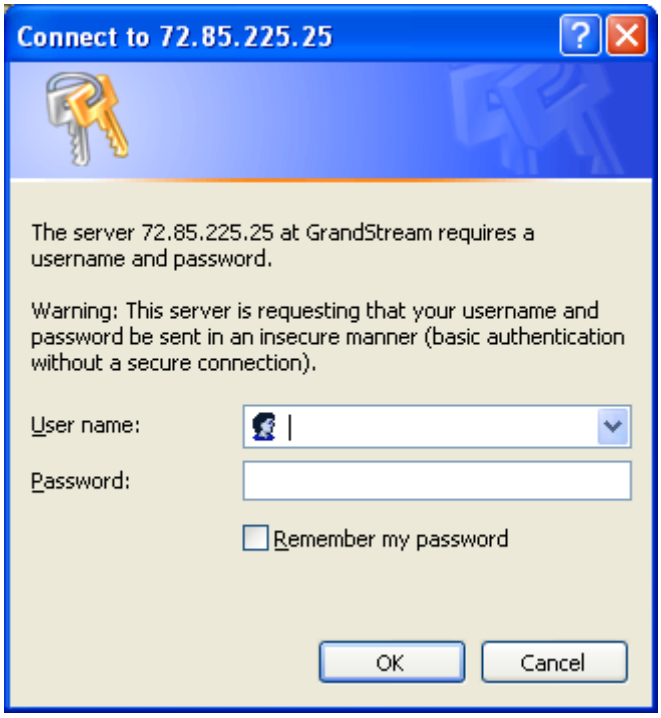
The receiver will hear a siren mentioning “something unusual happening in the monitored area”.

User can take several ways to verify what is happening “REALLY” in the monitored area:

1) Check the email and see the attached snapshot if SMTP is configured. (Search the JUNK mail folder to make sure that email is NOT blocked or put into junk mail).
2) Use “Browser” of the PC or Smartphone with Internet access to check back the live camera, if user configured the router with port forwarding correctly.
3) Call back to the PSTN line, after input the PIN code (if configured), the dial any digits with “#” key to “hear” what happened near the area where the microphone of surveillance device can work.
4) Take related action (like call law enforcement) to get help if it is true alarm or the situation required
5) If user has access to internet via PC or Smartphone, user can open the browser by input the correct URL (if DDNS is used) or the WAN IP address of the router (if port forwarding is configured), to check back and see and hear what is going on “LIVE” to the surveillance device. Detailed configurations please refer to the User Manual of the related surveillance product.

- Figure 3-1 below is the pop-up credential verification request from the surveillance device if correct URL/IP address input to the browser (Internet Explorer in the example)

Figure 3-1: Check back the Surveillance Device


Connect to 72.85.225.25
The server 72.85.225.25 at GrandStream requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
Password:
Remember my password
OK
Cancel

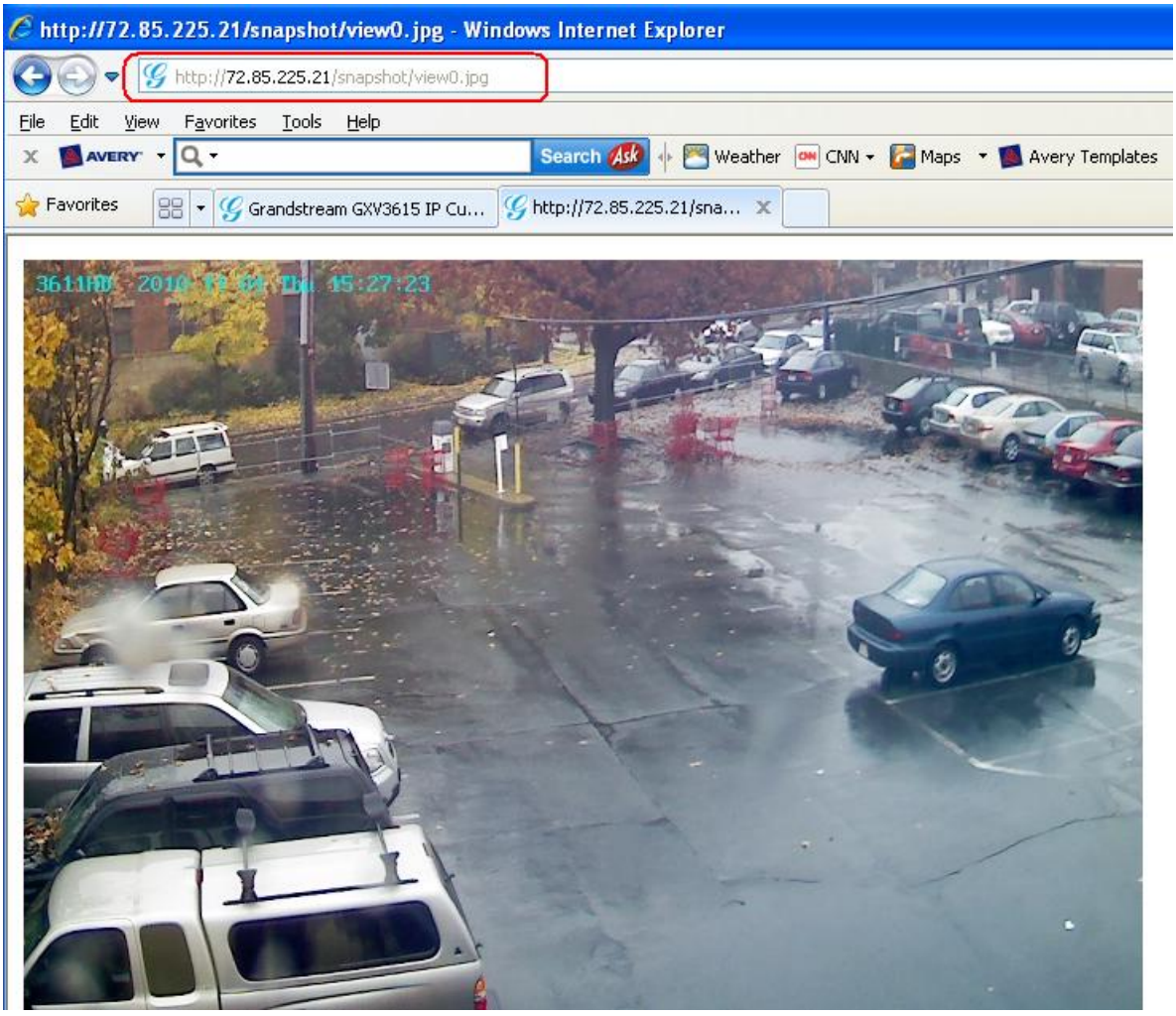
- Figure 3-2 below is screenshot of how the snapshot looks like.

This is best for user owing Smartphone but with limited data service. User just need to bookmark the URL or IP and whenever alarm call received, user can just open the browser to check the bookmarked page to see the snapshot of that surveillance device, if the router with correct Port Forwarding configured. Therefore the user only is charged by the Mobile Carrier for the data where the snapshot frame viewed.

The format of the URL command is:

http://IP.Address.of.SurveillianceDevice/snapshot/view0.jpg

Figure 3-2: Check Snapshot of the Surveillance Device



NOTE:

For how to configure the port forwarding in the router, please refer to the related User Manual of the router.